



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/503,181	02/14/2000	Yair Frankel	PM 265650	6203
909 7590 09/07/2007 PILLSBURY WINTHROP SHAW PITTMAN, LLP Eric S. Cherry - Docketing Supervisor P.O. BOX 10500 MCLEAN, VA 22102			EXAMINER LEMMMA, SAMSON B	
			ART UNIT 2132	PAPER NUMBER
			MAIL DATE 09/07/2007	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 09/503,181	Applicant(s) FRANKEL ET AL.	
	Examiner Samson B. Lemma	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 21 June 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-4 and 6-67 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-4 and 6-67 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

Art Unit: 2132

DETAILED ACTION

1. This office action is in reply to an amendment filed on June 21, 2007.
Claim 5 is canceled previously. Claims 1-4 and 6-67 are pending/examined.
2. All independent **claims namely, claims 1, 16 and 52** are amended.

Response to Arguments

3. Applicant's argument filed on June 21, 2007 have been fully considered but they are not persuasive.

Referring to independent claims, Applicant argued that limitations recited in the independent claims are not disclosed by the reference/s on the record namely by Ginter or Lampson individually or by the combinations of the reference/s.

Applicants submit the following in support of his argument.

*"In short, Ginter is directed to a specific computer system for secure handling of information. Ginter is simply **not directed to an organizational structure of one or more business organizations**, let alone directed to entities within an organizational structure of one or more business organizations (such as, without limitation, employees of a corporation) and the roles/functions (such as, without limitation, a president of a corporation) of entities within the organizational structure."*

Examiner disagrees with the above argument.

Examiner would point out that Ginter on Column 55, lines 33-43, the following is disclosed which meets the limitation recited as *"one or more business organizations."*

"Information utility" 200 in FIG. 1 can be a collection of participants that may act as distributors, financial clearinghouses, and administrators. FIG. 1A shows an example of what may be inside one example of information utility 200. Information utility **participants 200a-200g could each be an independent organization/business.**

There can be any number of each of participants 200a-200g. In this example, electronic

Art Unit: 2132

"switch" 200a connects internal parts of information utility 200 to each other and to outside participants, and may also connect outside participants to one another."

Furthermore, on column 303, lines 3-19, the following has been disclosed, which meets the limitation of "roles/functions in organizational structure."

*"In addition, the organization may desire to permit users to exercise control over specific documents for which the user has some defined responsibility. As an example, a user (the "originating user") may wish to place an "originator controlled" ("ORCON") restriction on a certain document, such that the document may be transmitted and used only by those specific other users whom he designates (and only in certain, expressly authorized ways). Such a restriction may be flexible if the "distribution list" could be modified after the creation of the document, specifically in the event of someone requesting permission from the originating user to transmit the document outside the original list of authorized recipients. **The originating user may wish to permit distribution only to specific users, defined groups of users, defined geographic areas, users authorized to act in specific organizational roles, or a combination of any or all such attributes.**"*

The rest of the argument is the same/similar to that of the previous argument, therefore the pervious relpy by the office is still applicable towards applicant's present argument.

For instance in the previous office action, applicant wrote the following remark.

"...the cited portions of Ginter et al. fail to disclose, teach, or suggest "organizing entities within the organizational structure as roles through associating the electronic representations of entities with electronic representations of roles".

Art Unit: 2132

"The references to "role" in the cited portions of Ginter et al. are simply inapposite to the claim language since the claim recites more than the word "roles". For example, none of the cited portions of Ginter et al. references an organizational structure or organizing entities within that organizational structure by associating the electronic representations of entities with electronic representations of roles. Rather, the cited portions of Ginter et al. merely indicate the participants in the electronic commerce system of Ginter et al. may adopt different roles but provide no disclosure, teaching or suggestion of organizing entities, which have associated cryptographic capabilities, within an organizational structure, let alone organizing those entities by associating corresponding electronic representations as recited in claim 1."

Examiner disagrees with the above argument.

The Applicant has recited a method of control and maintenance of an operation organizational structure where various entities are associated with particular roles.

As the office pointed out above Ginter et al discloses that ***user may wish to permit distribution only to specific users, defined groups of users, defined geographic areas, users authorized to act in specific organizational roles, or a combination of any or all such attributes.***"/[See at least column 303, lines 3-19]

Furthermore as it is explained in the previous office action,

Ginter et al. discloses a massive commercial and organizational structure with cryptographic capabilities with a number of modules interacting. Ginter et al. is in essence, a complete cryptographic system disclosed with detail. The Applicant's central argument appears to be grounded around the assertion that

"...none of the cited portions of Ginter et al. references an organizational structure or organizing entities within that organizational structure by associating the electronic representations of entities with electronic representations of roles."

Art Unit: 2132

It is the office's position however that any cryptographic entity enabled in the technological arts, be it a smartcard system, a general client server authentication system, or an encrypted transaction system may be construed as an "organizational structure."

It is furthermore the Examiner's position that any modules or subparts that server to enable the technological realization of a functional organization may be construed as an assignment of "roles" to these modules insofar as their functions, and therefore contribution to the organizational entity, dictate.

An organization is simply an aggregation of interacting persons, or components to impel a specified directive or purpose. The interactions of these components with respect to that organization in forwarding that purpose has been construed by the Examiner to be their "role." In response to the Applicant's additional contention that Ginter et al. provides *no disclosure, teaching or suggestion of organizing entities, which have associated cryptographic capabilities, within an organizational structure, let alone organizing those entities by associating corresponding electronic representations*, it is the Examiner's position that the cryptographic modules of Ginter et al. in the rejection below recite these limitations and their organization by corresponding electronic representations embodied by their realization in Ginter et al by virtue of their enablement in the technological arts.

For Example, paragraphs 1500-1502 of Ginter et al. disclose the usage of cryptographic keys in a "compare block" 3362A of Figure 67a. These cryptographic keys are further identified by Ginter et al. in paragraph 1502 as "important data structures." This reads upon the Applicant's limitation of organizing entities with

Art Unit: 2132

cryptographic capabilities with by associating corresponding electronic representations.

In this case, the associating corresponding electronic representation is the data structure representing the cryptographic keys.

(1500) A further attack technique in this example might involve comparing installed operational material 3472 software and data files among several different PPE 650 instances to identify important data structures, such as cryptographic keys (see "compare" block 3362A of FIG. 67A; and FIG. 67B, block 3362). The resulting list of differences 3362B could be carefully analyzed (see FIG. 67A's magnifying glass 3362C) to obtain important clues, using analysis techniques such as described above.

(1501) A further attack technique might involve comparing the memory and/or disk images of installed operational material 3472 software and data files in a single instance of PPE 650, after performing various operations using the PPE. This could serve to identify important data structures, such as cryptographic keys (see "compare" block 3362A of FIG. 67A; and FIG. 67B, block 3362). The resulting list of differences 3362B could be carefully analyzed (see FIG. 67A's magnifying glass 3362C) to obtain important clues, using analysis techniques such as described above.

(1502) A further attack technique might involve analyzing the timing and/or order of modification to memory and/or disk images of installed operational material 3472 software and data files in a single instance of PPE 650, during the performance performing various operations using the PPE. This could serve to identify important data structures, such as cryptographic keys (see "compare" block 3362A of FIG. 67A; and FIG. 67B, block 3362). The resulting list of differences 3362B could be carefully analyzed (see FIG. 67A's magnifying glass 3362C) to obtain important clues, using analysis techniques such as described above.

Claim 16 recites a system "comprising code executable by a computing device." In light of the specification and claim 1, which recites "the method being automated using a computing device", the Examiner has interpreted the preamble recitation to include the computing device because it "breathes life and meaning into the claim" in accordance with MPEP 2111.02

Art Unit: 2132

With respect to the Applicant's arguments of the rejections under 35 USC 103, Applicant's arguments have been fully considered but are not also persuasive.

Referring to the independent claims 16, applicant first argued that the primary and secondary reference/s used in rejecting the claims pertain to significantly different fields of endeavor.

Examiner disagrees with the above argument for the simple reason that Lampson, the primary reference on the record, is directed to Authentication, in Distributed systems, Theory and Practice and the secondary reference on the record namely Ginter is directed to the systems and methods for secure transaction management and electronic rights protections. Thus, both are directed and focuses on the field of "computer security and cryptography".

Examiner could not understand how and why these two references are from different fields of endeavors.

Furthermore, In response to applicant's above argument that the secondary reference Ginter is nonanalogous art, it has been held that a prior art reference must either be in the field of applicant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the applicant was concerned, in order to be relied upon as a basis for rejection of the claimed invention. See *In re Oetiker*, 977 F.2d 1443, 24 USPQ2d 1443 (Fed. Cir. 1992). In this case, both references are directed and focuses on the field of "computer security and cryptography" and are indeed in the field of applicant's endeavor.

Referring to the independent claim 16, Applicant further presented the following argument.

"None of the cited portions of Ginter discuss change of maintained electronic representations of entities within a business organization, or of characteristics (such as an entity's size, threshold for a quorum, or visibility (see. e.g., page 21 of the

Art Unit: 2132

specification)) of entities within a business organization, or of relationships of entities within a business organization, let alone to do so upon any addition, deletion or modification of a characteristic or relationship of entities within a business organization."

Examiner disagrees with the above argument.

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e. characteristics such as an entity's size, threshold for a quorum, or visibility...,) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

However, Examiner would point that the secondary reference on the record, Ginter et al, explicitly discloses an electronic embodiment of a system for control and maintenance of an operational structure including "changing the maintained electronic representation of said entities said characteristics and said relationships upon an addition, deletion or modification of a characteristic or relationship of the entities." paragraphs 164, 204, 209, 206

Ginter, paragraph 164

(164) VDEF transaction control elements reflect and enact content specific and/or more generalized administrative (for example, general operating system) control information. VDEF capabilities which can generally take the form of applications (application models) that have more or less configurability which can be shaped by VDE participants, through the use, for example, of VDE templates, to employ specific capabilities, along, for example, with capability parameter data to reflect the elements of one or more express electronic agreements between VDE participants in regards to the use of electronic content such as commercially distributed products. These control capabilities manage the use of, and/or auditing of use of, electronic content, as well as reporting information based upon content use, and any payment for said use. VDEF capabilities may "evolve" to reflect the requirements of one or more successive parties who receive or otherwise contribute to a given set of control information. Frequently, for a VDE application for a given content model (such as distribution of entertainment on CD-ROM, content delivery from an Internet repository, or electronic catalog shopping and advertising, or some combination of the above) participants would be able to securely select from amongst available, alternative control methods and apply related parameter data,

Art Unit: 2132

wherein such selection of control method and/or submission of data would constitute their "contribution" of control information. Alternatively, or in addition, certain control methods that have been expressly certified as securely interoperable and compatible with said application may be independently submitted by a participant as part of such a contribution. In the most general example, a generally certified load module (certified for a given VDE arrangement and/or content class) may be used with many or any VDE application that operates in nodes of said arrangement. These parties, to the extent they are allowed, can independently and securely add, delete, and/or otherwise modify the specification of load modules and methods, as well as add, delete or otherwise modify related information.

Ginter paragraph 204

Handlers in a pathway of handling of content control information, to the extent each is authorized, can establish, modify, and/or contribute to, permission, auditing, payment, and reporting control information related to controlling, analyzing, paying for, and/or reporting usage of, electronic content and/or appliances (for example, as related to usage of VDE controlled property content). Independently delivered (from an independent source which is independent except in regards to certification), at least in part secure, control information can be employed to securely modify content control information when content control information has flowed from one party to another party in a sequence of VDE content control information handling. This modification employs, for example, one or more VDE component assemblies being securely processed in a VDE secure subsystem.

Referring to independent claim 52, Applicant further presented the following argument.

"Thus none of the cited portions of Ginter would disclose or teach the claimed database, let alone a maintenance system to maintain coordination between the database and cryptographic capabilities (which is not even referenced in the cited portions)."

Examiner disagrees with the above argument.

Even though applicant's is correct that the cited portion does not explicitly mention the database the feature is already disclosed by the reference preceding the citation. For instance, Examiner would like to point out that **Ginter on column 8, lines 1-7** discloses the following.

Art Unit: 2132

"VDE normally employs an integration of cryptographic and other security technologies (e.g. encryption, digital signatures, etc.), **with other technologies including: component, distributed, and event driven operating system technology, and related communications, object container, database, smart agent, smart card, and semiconductor design technologies.**"

Furthermore, for the 103 rejection, applicant's arguments against the references individually, Examiner would indicate that one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

As to the argument made to the rest of the dependent claims, Examiner would point out that the dependent claims stands and falls with the corresponding independent claims.

Therefore all limitations recited in the body of independent claims are undoubtedly disclosed by the reference/s on the record and the rejection is maintained until the applicant amends the respective independent claims and successfully overcome the rejection without introducing new matters.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless -

Art Unit: 2132

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1-15, 64-65 are rejected under 35 U.S.C. 102(e) as being anticipated by Ginter et al., US patent 5892900.

In reference to claim 1:

Ginter et al. discloses a method for control and maintenance of an operational organization structure(Figure 1), involving cryptographic control and maintenance of entities within one or more business organizations(Figures 1 and 1A),

(Ginter on Column 55, lines 33-43, the following is disclosed which meets the limitation recited as "one or more business organizations." "Information utility" 200 in FIG. 1 can be a collection of participants that may act as distributors, financial clearinghouses, and administrators. FIG. 1A shows an example of what may be inside one example of information utility 200. Information utility participants 200a-200g could each be an independent organization/business. There can be any number of each of participants 200a-200g. In this example, electronic "switch" 200a connects internal parts of information utility 200 to each other and to outside participants, and may also connect outside participants to one another.)

the method being automated using a computing device(Column 4, lines 48-62) & (Figure 1A, Items 200e, 200h), the method comprising:

Art Unit: 2132

- **Associating electronic representations of entities with cryptographic capabilities;** (Column 9, lines 3-33), paragraphs 710, 1282-1284, 1289

(710) SPE 503/HPE 655 may support both Public Key type keys and Bulk Encryption type keys. The public key (PK) encryption type keys stored by SPU 500 and managed by key and tag manager 558 may include, for example, a device public key, a device private key, a PK certificate, and a public key for the certificate. Generally, public keys and certificates can be stored externally in non-secured memory if desired, but the device private key and the public key for the certificate should only be stored internally in an SPU 500 EEPROM or NVRAM 534b. Some of the types of bulk encryption keys used by the SPU 500 may include, for example, general-purpose bulk encryption keys, administrative object private header keys, stationary object private header keys, traveling object private header keys, download/initialization keys, backup keys, trail keys, and management file keys.

(1282) Conventional techniques for generating PK and non-PK keys based upon such "seeds" may be used. Thus, if performance and manufacturing costs permit, PPE 650 in the preferred embodiment will generate its own public/private key pair based on such random or pseudo-random "seed" values. This key pair may then be used for external communications between the PPE 650 that generated the key pair and other PPEs that wish to communicate with it. For example, the generating PPE 650 may reveal the public key of the key pair to other PPEs. This allows other PPEs 650 using the public key to encrypt messages that may be decrypted only by the generating PPE (the generating PPE is the only PPE that "knows" the corresponding "private key"). Similarly, the generating PPE 650 may encrypt messages using its private key that, when decrypted successfully by other PPEs with the generating PPE's public key, permit the other PPEs to authenticate that the generating PPE sent the message.

(1283) Before one PPE 650 uses a public key generated by another PPE, a public key certification process should be used to provide authenticity certificates for the public key. A public-key certificate is someone's public key "signed" by a trustworthy entity such as an authentic PPE 650 or a VDE administrator. Certificates are used to thwart attempts to convince a PPE 650 that it is communicating with an authentic PPE when it is not (e.g., it is actually communicating with a person attempting to break the security of PPE 650). One or more VDE administrators in the preferred embodiment may constitute a certifying authority. By "signing" both the public key generated by a PPE 650 and information about the PPE and/or the corresponding VDE electronic appliance 600 (e.g., site ID, user ID, expiration date, name, address, etc.), the VDE administrator certifying authority can certify that information about the PPE and/or the VDE electronic appliance is correct and that the public key belongs to that particular VDE mode.

(1284) Certificates play an important role in the trustedness of digital

Art Unit: 2132

signatures, and also are important in the public-key authentication communications protocol (to be discussed below). In the preferred embodiment, these certificates may include information about the trustedness/level of security of a particular VDE electronic appliance 600 (e.g., whether or not it has a hardware-based SPE 503 or is instead a less trusted software emulation type HPE 655) that can be used to avoid transmitting certain highly secure information to less trusted/secure VDE installations.

(1289) In the preferred embodiment, PPE 650 may generate its own certificate, or the certificate may be obtained externally, such as from a certifying authority VDE administrator. Irrespective of where the digital certificate is generated, the certificate is eventually registered by the VDE administrator certifying authority so that other VDE electronic appliances 600 may have access to (and trust) the public key. For example, PPE 650 may communicate its public key and other information to a certifying authority which may then encrypt the public key and other information using the certifying authority's private key. Other installations 600 may trust the "certificate" because it can be authenticated by using the certifying authority's public key to decrypt it. As another example, the certifying authority may encrypt the public key it receives from the generating PPE 650 and use it to encrypt the certifying authority's private key. The certifying authority may then send this encrypted information back to the generating PPE 650. The generating PPE 650 may then use the certifying authority's private key to internally create a digital certificate, after which it may destroy its copy of the certifying authority's private key. The generating PPE 650 may then send out its digital certificate to be stored in a certification repository at the VDE administrator (or elsewhere) if desired. The certificate process can also be implemented with an external key pair generator and certificate generator, but might be somewhat less secure depending on the nature of the secure facility. In such a case, a manufacturing key should be used in PPE 650 to limit exposure to the other keys involved.

• **Organizing entities within the organizational structure as roles through associating the electronic representations of entities with electronic representations of roles;** (On column 303, lines 3-19, the following has been disclosed, which meets the limitation of "roles/functions in organizational structure."

"In addition, the organization may desire to permit users to exercise control over specific documents for which the user has some defined responsibility. As an example, a user (the "originating user") may wish to place an "originator controlled" ("ORCON") restriction on a certain document, such that the document may be transmitted and used only by those specific other users whom he designates (and only in certain, expressly

Art Unit: 2132

authorized ways). Such a restriction may be flexible if the "distribution list" could be modified after the creation of the document, specifically in the event of someone requesting permission from the originating user to transmit the document outside the original list of authorized recipients. The originating user may wish to permit distribution only to specific users, defined groups of users, defined geographic areas, users authorized to act in specific organizational roles, or a combination of any or all such attributes." See also Figures 1, 1A, 2, and paragraph 1865 and 1866)

(1865) All participants of VDE 100 have the innate ability to participate in any role. For example, users may gather together existing protected packages, add (create new content) packages of their own, and create new products. They may choose to serve as their own distributor, or delegate this responsibility to others. These capabilities are particularly important in the object oriented paradigm which is entering the marketplace today. The production of compound objects, object linking and embedding, and other multi-source processes will create a need for these capabilities of VDE 100. The distribution process provided by VDE 100 is symmetrical; any end-user may redistribute information received to other end-users, provided they possess permission from and follow the rules established by the distribution chain VDE control information governing redistribution. End-users also may, within the same rules and permissions restriction, encapsulate content owned by others within newly published works and distribute these works independently. Royalty payments for the new works may be accessed by the publisher, distributors, or end-users, and may be tracked and electronically collected at any stage of the chain.

(1866) Independent financial providers can play an important role in VDE 100. The VDE financial provider role is similar to the role played by organizations such as VISA in traditional distribution scenarios. In any distribution model, authorizing payments for use of products or services and auditing usage for consistency and irregularities, is critical. In VDE 100, these are the roles filled by independent financial providers. The independent financial providers may also provide audit services to content providers. Thus, budgets or limits on use, and audits, or records of use, may be processed by (and may also be put in place by) clearinghouses 116, and the clearinghouses may then collect usage payments from users 112. Any VDE user 112 may assign the right to process information or perform services on their behalf to the extent allowed by senior control information. The arrangement by which one VDE participant acts on behalf of another is called a "proxy." Audit, distribution, and other important rights may be "proxied" if permitted by the content provider. One special type of "proxy" is the VDE administrator 116b. A VDE administrator is an organization (which may be acting also as a financial clearinghouse 116) that has permission to manage (for example, "intervene" to reset) some portion or all of VDE secure subsystem control information for VDE electronic appliances. This administration right may extend only to admitting new appliances to a VDE

Art Unit: 2132

infrastructure and to recovering "crashed" or otherwise inoperable appliances, and providing periodic VDE updates.

- Upon any addition, deletion, or modification of an entity, a cryptographic capability, or any of their associations, maintaining roles within the organizational structure by adding, deleting or modifying electronic representations of the entities, cryptographic capabilities, roles, or any of their associations. (Column 13, lines 25-50) and paragraphs 164, 204, 209, 206

Ginter, paragraph 164

(164) VDEF transaction control elements reflect and enact content specific and/or more generalized administrative (for example, general operating system) control information. VDEF capabilities which can generally take the form of applications (application models) that have more or less configurability which can be shaped by VDE participants, through the use, for example, of VDE templates, to employ specific capabilities, along, for example, with capability parameter data to reflect the elements of one or more express electronic agreements between VDE participants in regards to the use of electronic content such as commercially distributed products. These control capabilities manage the use of, and/or auditing of use of, electronic content, as well as reporting information based upon content use, and any payment for said use. VDEF capabilities may "evolve" to reflect the requirements of one or more successive parties who receive or otherwise contribute to a given set of control information. Frequently, for a VDE application for a given content model (such as distribution of entertainment on CD-ROM, content delivery from an Internet repository, or electronic catalog shopping and advertising, or some combination of the above) participants would be able to securely select from amongst available, alternative control methods and apply related parameter data, wherein such selection of control method and/or submission of data would constitute their "contribution" of control information. Alternatively, or in addition, certain control methods that have been expressly certified as securely interoperable and compatible with said application may be independently submitted by a participant as part of such a contribution. In the most general example, a generally certified load module (certified for a given VDE arrangement and/or content class) may be used with many or any VDE application that operates in nodes of said arrangement. These parties, to the extent they are allowed, can independently and securely add, delete, and/or otherwise modify the specification of load modules and methods, as well as add,

Art Unit: 2132

delete or otherwise modify related information.

Ginter paragraph 204

Handlers in a pathway of handling of content control information, to the extent each is authorized, can establish, modify, and/or contribute to, permission, auditing, payment, and reporting control information related to controlling, analyzing, paying for, and/or reporting usage of, electronic content and/or appliances (for example, as related to usage of VDE controlled property content). Independently delivered (from an independent source which is independent except in regards to certification), at least in part secure, control information can be employed to securely modify content control information when content control information has flowed from one party to another party in a sequence of VDE content control information handling. This modification employs, for example, one or more VDE component assemblies being securely processed in a VDE secure subsystem.

Ginter paragraph 209

(209) (a) "evolve," for example, the extractor of content may add new control methods and/or modify control parameter data, such as VDE application compliant methods, to the extent allowed by the content's in-place control information. Such new control information might specify, for example, who may use at least a portion of the new object, and/or how said at least a portion of said extracted content may be used (e.g. when at least a portion may be used, or what portion or quantity of portions may be used);

Ginter paragraph 306

(306) ROS 602 provided by the preferred embodiment permits secure modification and update of control information governing each component. The control information may be provided in a template format such as method options to an end-user. An end-user may then customize the actual control information used within guidelines provided by a distributor or content creator. Modification and update of existing control structures is preferably also a controllable event subject to auditing and control information.

In reference to claim 2:

Ginter et al. (paragraph 1289) discloses a method as in claim 1, wherein the method involves at least a public key infrastructure operation.

Art Unit: 2132

In reference to claim 3:

Ginter et al. discloses a method as in claim 1 wherein the control and maintenance further comprises:

Assigning elements in said organizational structure to roles within said organizational structure. (Figures 2 and 5B) & paragraph 1866.

In reference to claim 4:

Ginter et al. (Figures 1 and 1A) & paragraphs 1885, 1886, 1887 discloses a method as in claim 1 wherein the control and maintenance further comprises:

Assigning elements in said organizational structure to groups within said organizational structure.

(1885) A VDE node electronic appliance 600 may receive and process audit records on behalf of an object provider if that VDE node receives any necessary administrative budget, audit method, and audit key information (used, for example, to decrypt audit trails), from the object provider. An auditing-capable VDE electronic appliance 600 may control execution of audit reduction methods. "Audit reduction" in the preferred embodiment is the process of extracting information from audit records and/or processes that an object provider (e.g., any object provider along a chain of handling of the object) has specified to be reported to an object's distributors, object creators, client administrators, and/or any other user of audit information. This may include, for example, advertisers who may be required to pay for a user's usage of object content. In one embodiment, for example, a clearinghouse can have the ability to "append" budget, audit method, and/or audit key information to an object or class or other grouping of objects located at a user site or located at an object provider site to ensure that desired audit processes will take place in a "trusted" fashion. A participant in a chain of handling of a VDE content container and/or content container control information object may act as a "proxy" for another party in a chain of handling of usage auditing information related to usage of object content (for example a clearinghouse, an advertiser, or a party interested in market survey

Art Unit: 2132

and/or specific customer usage information). This may be done by specifying, for that other party, budget, audit method, and/or key information that may be necessary to ensure audit information is gathered and/or provided to, in a proper manner, said additional party. For example, employing specification information provided by said other party.

(1886) Object Creation and Initial Control Structures

(1887) The VDE preferred embodiment object creation and control structure design processes support fundamental configurability of control information. This enables VDE 100 to support a full range of possible content types, distribution pathways, usage control information, auditing requirements, and users and user groups. VDE object creation in the preferred embodiment employs VDE templates whose atomic elements represent at least in part modular control processes. Employing VDE creation software (in the preferred embodiment a GUI programming process) and VDE templates, users may create VDE objects 300 by, for example, partitioning the objects, placing "meta data" (e.g., author's name, creation date, etc.) into them, and assigning rights associated with them and/or object content to, for example, a publisher and/or content creator. When an object creator runs through this process, she normally will go through a content specification procedure which will request required data. The content specification process, when satisfied, may proceed by, for example, inserting data into a template and encapsulating the content. In addition, in the preferred embodiment, an object may also automatically register its presence with the local VDE node electronic appliance 600 secure subsystem, and at least one permissions record 808 may be produced as a result of the interaction of template instructions and atomic methods, as well as one or more pieces of control structure which can include one or more methods, budgets, and/or etc. A registration process may require a budget to be created for the object. If an object creation process specifies an initial distribution, an administrative object may also be created for distribution. The administrative object may contain one or more permission records 808, other control structures, methods, and/or load modules.

Claim 5 has been canceled.

In reference to claim 6:

Ginter et al. (Figures 1 and 1A) & paragraphs 1885, 1886, 1887 discloses a method as in claim 3 wherein at least some of said elements are already grouped elements, where the previously grouped elements include user groups.

Art Unit: 2132

In reference to claim 7:

Ginter et al. paragraphs 986, 1012, 1989, and 2006 discloses a method as in claim 1 wherein said method involves access control technology.

(986) In the example, subject table 462 associates users (or groups of users) with registered objects. The example subject table 462 performs the function of an access control list by specifying which users are authorized to access which registered VDE objects 300.

(1012) User or user group ID 472(2) identifies a user or a user group authorized to use the object identified in field 468(5). Thus, the fields 468(5) and 472(2) together form the heart of the access control list provided by subject table 462. User attributes field 472(3) may specify attributes pertaining to use/access to object 300 by the user or user group specified in fields 472(2). Any number of different users or user groups may be added to the access control list (each with a different set of attributes 472(3)) by providing additional subject records 470 in the "linked list" structure.

(1989) In this example, the law firm receives in VDE content containers documents from their client's VDE installation secure subsystem(s). Alternatively, or in addition, the law firm may receive either physical documents which may be scanned into electronic form, and/or they receive electronic documents which have not yet been placed in VDE containers. The electronic form of a document is stored as a VDE container (object) associated with the specific client and/or case. The VDE container mechanism supports a hierarchical ordering scheme for organizing files and other information within a container; this mechanism may be used to organize the electronic copies of the documents within a container. A VDE container is associated with specific access control information and rights that are described in one or more permissions control information sets (PERCs) associated with that container. In this example, only those members of the law firm who possess a VDE instance, an appropriate PERC, and the VDE object that contains the desired document, may use the document. Alternatively or in addition, a law firm member may use a VDE instance which has been installed on the law firm's network server. In this case, the member must be identified by an appropriate PERC and have access to the document containing VDE object (in order to use the server VDE installation). Basic access control to electronic documents is enabled using the secure subsystem of one or more user VDE installations.

(2006) The organization as a whole may have a well-defined policy for access control to, and/or other usage control of documents. This policy may be based

Art Unit: 2132

on a "lattice model" of information flow, in which documents are characterized as having one or more hierarchical "classification" security attributes 9903 and zero or more non-hierarchical "compartment" security attributes, all of which together comprise a sensitivity security attribute.

In reference to claim 8:

Ginter et al. paragraphs 986, 1012, 1989, and 2006 discloses a method as in claim 1, wherein said method involves at least an access control operation.

In reference to claim 9:

Ginter et al. discloses a method as in claim 1 wherein said method involves at least a data-base operation. (Figure 12, Item 730, Item 750, 744, 752) and paragraph 104

(104) Secondary storage 652 in this example stores code and data used by CPU 654 and/or SPU 500 to control the overall operation of electronic appliance 600. For example, FIG. 8 shows that "Rights Operating System" ("ROS") 602 (including a portion 604 of ROS that provides VDE functions and a portion 606 that provides other OS functions) shown in FIG. 7 may be stored on secondary storage 652. Secondary storage 652 may also store one or more VDE objects 300. FIG. 8 also shows that the secure files 610 shown in FIG. 7 may be stored on secondary storage 652 in the form of a "secure database" or management file system 610. This secure database 610 may store and organize information used by ROS 602 to perform VDE functions 604. Thus, the code that is executed to perform VDE and other OS functions 604, 606, and secure files 610 (as well as VDE objects 300) associated with those functions may be stored in secondary storage 652. Secondary storage 652 may also store "other information" 673 such as, for example, information used by other operating system functions 606 for task management, non-VDE files, etc. Portions of the elements indicated in secondary storage 652 may also be stored in ROM 658, so long as those elements do not require changes (except when ROM 658 is replaced). Portions of ROS 602 in particular may desirably be included in ROM 658 (e.g., "bootstrap" routines, POST routines, etc. for use in establishing an operating environment for electronic appliance 600 when power is applied).

Art Unit: 2132

In reference to claim 10:

Ginter et al. discloses a method as in claim 1 wherein said method involves at least one operation implemented in a hardware device. (Figures 12, 12a) and paragraph 104

In reference to claim 11:

Ginter et al. discloses a method as in claim 1, wherein the operational organizational structure represents at least one commercial organization. (Figures 1 and 1a) and paragraph 1866

(1866) Independent financial providers can play an important role in VDE 100. The VDE financial provider role is similar to the role played by organizations such as VISA in traditional distribution scenarios. In any distribution model, authorizing payments for use of products or services and auditing usage for consistency and irregularities, is critical. In VDE 100, these are the roles filled by independent financial providers. The independent financial providers may also provide audit services to content providers. Thus, budgets or limits on use, and audits, or records of use, may be processed by (and may also be put in place by) clearinghouses 116, and the clearinghouses may then collect usage payments from users 112. Any VDE user 112 may assign the right to process information or perform services on their behalf to the extent allowed by senior control information. The arrangement by which one VDE participant acts on behalf of another is called a "proxy." Audit, distribution, and other important rights may be "proxied" if permitted by the content provider. One special type of "proxy" is the VDE administrator 116b. A VDE administrator is an organization (which may be acting also as a financial clearinghouse 116) that has permission to manage (for example, "intervene" to reset) some portion or all of VDE secure subsystem control information for VDE electronic appliances. This administration right may extend only to admitting new appliances to a VDE infrastructure and to recovering "crashed" or otherwise inoperable appliances, and providing periodic VDE updates.

In reference to claim 12:

Ginter et al. discloses a method as in claim 1 wherein the operational organizational structure represents at least two organizations, and wherein one of said organizations performs at

Art Unit: 2132

least one function on behalf of another of said organizations.

(Figures 1 and 1a)

In reference to claim 13:

Ginter et al. (paragraph 251) discloses a method as in claim 1 wherein the method further comprises changing software whose authorization is checked.

(251) The updating of property management files at each location of a VDE arrangement, to accommodate new or modified control information, is performed in the VDE secure subsystem and under the control of secure management file updating programs executed by the protected subsystem. Since all secure communications are at least in part encrypted and the processing inside the secure subsystem is concealed from outside observation and interference, the present invention ensures that content control information can be enforced. As a result, the creator and/or distributor and/or client administrator and/or other contributor of secure control information for each property (for example, an end-user restricting the kind of audit information he or she will allow to be reported and/or a financial clearinghouse establishing certain criteria for use of its credit for payment for use of distributed content) can be confident that their contributed and accepted control information will be enforced (within the security limitations of a given VDE security implementation design). This control information can determine, for example:

In reference to claim 14:

Ginter et al. (Figures 1, 1A, paragraphs 145,226) discloses a method as in claim 1 wherein the method further comprises changing hardware.

(145) An objective of VDE is supporting a transaction/distribution control standard. Development of such a standard has many obstacles, given the security requirements and related hardware and communications issues, widely differing environments, information types, types of information usage, business and/or data security goals, varieties of participants, and properties of delivered information. A significant feature of VDE accommodates the many,

Art Unit: 2132

varying distribution and other transaction variables by, in part, decomposing electronic commerce and data security functions into generalized capability modules executable within a secure hardware SPU and/or corresponding software subsystem and further allowing extensive flexibility in assembling, modifying, and/or replacing, such modules (e.g. load modules and/or methods) in applications run on a VDE installation foundation. This configurability and reconfigurability allows electronic commerce and data security participants to reflect their priorities and requirements through a process of iteratively shaping an evolving extended electronic agreement (electronic control model). This shaping can occur as content control information passes from one VDE participant to another and to the extent allowed by "in place" content control information. This process allows users of VDE to recast existing control information and/or add new control information as necessary (including the elimination of no longer required elements).

(226) support the use of multiple VDE secure subsystems in a single VDE installation. Various security and/or performance advantages may be realized by employing a distributed VDE design within a single VDE installation. For example, designing a hardware based VDE secure subsystem into an electronic appliance VDE display device, and designing said subsystem's integration with said display device so that it is as close as possible to the point of display, will increase the security for video materials by making it materially more difficult to "steal" decrypted video information as it moves from outside to inside the video system. Ideally, for example, a VDE secure hardware module would be in the same physical package as the actual display monitor, such as within the packaging of a video monitor or other display device, and such device would be designed, to the extent commercially practical, to be as tamper resistant as reasonable. As another example, embedding a VDE hardware module into an I/O peripheral may have certain advantages from the standpoint of overall system throughput. If multiple VDE instances are employed within the same VDE installation, these instances will ideally share resources to the extent practical, such as VDE instances storing certain control information and content and/or appliance usage information on the same mass storage device and in the same VDE management database.

In reference to claim 15:

Ginter et al. (Figures 1, 1A, paragraph 1654, 1655) discloses a method as in claim 1 wherein the method further comprises moving hardware, where the hardware may be positioned to the liking of the user, such as the movement of the keyboard.

(1654) Although each of electronic appliances 600 shown in the figure may

Art Unit: 2132

have a generally similar architecture, they may perform different specialized tasks. For example, electronic appliance 600(1) might comprise a central processing section of a workstation responsible for managing the overall operation of the workstation and providing computation resources. Electronic appliance 600(2) might be a mass storage device 620 for the same workstation, and could provide a storage mechanism 2636 that might, for example, read information from and write information to a secondary storage device 652. Electronic appliance 600(3) might be a display device 614 responsible for performing display tasks, and could provide a displaying mechanism 2638 such as a graphics controller and associated video or other display. Electronic appliance 600(N) might be a printer 622 that performs printing related tasks and could include, for example, a print mechanism 2640.

(1655) Each of electronic appliances 600(1), . . . 600(N) could comprise a different module of the same workstation device all contained within a common housing, or the different electronic appliances could be located within different system components. For example, electronic appliance 600(2) could be disposed within a disk controller unit, electronic appliance 600(3) could be disposed within a display device 614 housing, and the electronic appliance 600(N) could be disposed within the housing of a printer 622. Referring back to FIG. 7, scanner 626, modem 618, telecommunication means 624, keyboard 612 and/or voice recognition box 613 could each comprise a VDE electronic appliance 600 having its own SPU 500. Additional examples include RF or otherwise wireless interface controller, a serial interface controller, LAN controllers, MPEG (video) controllers, etc.

In reference to claim 64:

Ginter et al. (Figures 1 and 1A) discloses a method as in claim 1 where a plurality of entities are electronically visible to one part of the organization, a first set of outside viewers, or both, and roles or characteristics thereof are electronically visible to another part of the organization, a second set of outside viewers, or both, where the plurality of entities are visible to VDE participant 1, and participant N.

Art Unit: 2132

In reference to claim 65:

Ginter et al. (paragraph 1866) discloses a method as in claim 1 where maintaining of roles within the organizational structure is protected and can be performed only by an authorized party inside or outside the organization, where the authorized party is the administrator.

(1866) Independent financial providers can play an important role in VDE 100. The VDE financial provider role is similar to the role played by organizations such as VISA in traditional distribution scenarios. In any distribution model, authorizing payments for use of products or services and auditing usage for consistency and irregularities, is critical. In VDE 100, these are the roles filled by independent financial providers. The independent financial providers may also provide audit services to content providers. Thus, budgets or limits on use, and audits, or records of use, may be processed by (and may also be put in place by) clearinghouses 116, and the clearinghouses may then collect usage payments from users 112. Any VDE user 112 may assign the right to process information or perform services on their behalf to the extent allowed by senior control information. The arrangement by which one VDE participant acts on behalf of another is called a "proxy." Audit, distribution, and other important rights may be "proxied" if permitted by the content provider. One special type of "proxy" is the VDE administrator 116b. A VDE administrator is an organization (which may be acting also as a financial clearinghouse 116) that has permission to manage (for example, "intervene" to reset) some portion or all of VDE secure subsystem control information for VDE electronic appliances. This administration right may extend only to admitting new appliances to a VDE infrastructure and to recovering "crashed" or otherwise inoperable appliances, and providing periodic VDE updates.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a

Art Unit: 2132

whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 16-63, 66-67 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lampson et al. and Ginter et al.

In reference to claim 16:

Lampson et al. discloses a system for control and maintenance of an operational structure involving at least:

- **one cryptographic method, where the cryptographic method is public key cryptography (Section 4.1 - Section 4.4 p. 275-279)**
- **entities within a business organizations, characteristics of said entities and relationships between said entities, where the entities are principals. (Section 2. Concepts P.268)**
- **where the capabilities, functions, characteristics, and relationships of entities**

are maintained and changed, where the changing is done through statements, and the statements denote actions that principals can say (Section 3.1- Section 4, pages 271-274)

Lampson fails to disclose "changing the maintained electronic representation of said entities of a business organization said characteristics and said relationships upon an addition, deletion or modification of a characteristic or relationship of the entities."

Art Unit: 2132

Ginter et al. discloses an electronic embodiment of a system for control and maintenance of an operational structure including "changing the maintained electronic representation of said entities of a business organization said characteristics and said relationships upon an addition, deletion or modification of a characteristic or relationship of the entities." paragraphs 164, 204, 209, 206

Ginter, paragraph 164

(164) VDEF transaction control elements reflect and enact content specific and/or more generalized administrative (for example, general operating system) control information. VDEF capabilities which can generally take the form of applications (application models) that have more or less configurability which can be shaped by VDE participants, through the use, for example, of VDE templates, to employ specific capabilities, along, for example, with capability parameter data to reflect the elements of one or more express electronic agreements between VDE participants in regards to the use of electronic content such as commercially distributed products. These control capabilities manage the use of, and/or auditing of use of, electronic content, as well as reporting information based upon content use, and any payment for said use. VDEF capabilities may "evolve" to reflect the requirements of one or more successive parties who receive or otherwise contribute to a given set of control information. Frequently, for a VDE application for a given content model (such as distribution of entertainment on CD-ROM, content delivery from an Internet repository, or electronic catalog shopping and advertising, or some combination of the above) participants would be able to securely select from amongst available, alternative control methods and apply related parameter data, wherein such selection of control method and/or submission of data would constitute their "contribution" of control information. Alternatively, or in addition, certain control methods that have been expressly certified as securely interoperable and compatible with said application may be independently submitted by a participant as part of such a contribution. In the most general example, a generally certified load module (certified for a given VDE arrangement and/or content class) may be used with many or any VDE application that operates in nodes of said arrangement. These parties, to the extent they are allowed, can independently and securely add, delete, and/or otherwise modify the specification of load modules and methods, as well as add, delete or otherwise modify related information.

Art Unit: 2132

Ginter paragraph 204

Handlers in a pathway of handling of content control information, to the extent each is authorized, can establish, modify, and/or contribute to, permission, auditing, payment, and reporting control information related to controlling, analyzing, paying for, and/or reporting usage of, electronic content and/or appliances (for example, as related to usage of VDE controlled property content). Independently delivered (from an independent source which is independent except in regards to certification), at least in part secure, control information can be employed to securely modify content control information when content control information has flowed from one party to another party in a sequence of VDE content control information handling. This modification employs, for example, one or more VDE component assemblies being securely processed in a VDE secure subsystem.

Ginter paragraph 209

(209) (a) "evolve," for example, the extractor of content may add new control methods and/or modify control parameter data, such as VDE application compliant methods, to the extent allowed by the content's in-place control information. Such new control information might specify, for example, who may use at least a portion of the new object, and/or how said at least a portion of said extracted content may be used (e.g. when at least a portion may be used, or what portion or quantity of portions may be used);

Ginter paragraph 306

(306) ROS 602 provided by the preferred embodiment permits secure modification and update of control information governing each component. The control information may be provided in a template format such as method options to an end-user. An end-user may then customize the actual control information used within guidelines provided by a distributor or content creator. Modification and update of existing control structures is preferably also a controllable event subject to auditing and control information.

Ginter et al. teaches

(146) VDE supports trusted (sufficiently secure) electronic information distribution and usage control models for both commercial electronic content distribution and data security applications. It can be configured to meet the diverse requirements of a network of interrelated participants that may include content creators, content distributors, client administrators, end users, and/or clearinghouses and/or other content usage information users. These parties may constitute a network of participants involved in simple to complex electronic content dissemination, usage control, usage reporting, and/or usage payment. Disseminated content may include both originally provided and VDE

Art Unit: 2132

generated information (such as content usage information) and content control information may persist through both chains (one or more pathways) of content and content control information handling, as well as the direct usage of content. The configurability provided by the present invention is particularly critical for supporting electronic commerce, that is enabling businesses to create relationships and evolve strategies that offer competitive value. Electronic commerce tools that are not inherently configurable and interoperable will ultimately fail to produce products (and services) that meet both basic requirements and evolving needs of most commerce applications.

(147) VDE's fundamental configurability will allow a broad range of competitive electronic commerce business models to flourish. It allows business models to be shaped to maximize revenues sources, end-user product value, and operating efficiencies. VDE can be employed to support multiple, differing models, take advantage of new revenue opportunities, and deliver product configurations most desired by users. Electronic commerce technologies that do not, as the present invention does:

(148) support a broad range of possible, complementary revenue activities,

(149) offer a flexible array of content usage features most desired by customers, and

(150) exploit opportunities for operating efficiencies,

(151) will result in products that are often intrinsically more costly and less appealing and therefore less competitive in the marketplace.

(152) Some of the key factors contributing to the configurability intrinsic to the present invention include:

(153) (a) integration into the fundamental control environment of a broad range of electronic appliances through portable API and programming language tools that efficiently support merging of control and auditing capabilities in nearly any electronic appliance environment while maintaining overall system security;

(154) (b) modular data structures;

(155) (c) generic content model;

(156) (d) general modularity and independence of foundation architectural components;

(157) (e) modular security structures;

(158) (f) variable length and multiple branching chains of control; and

(159) (g) independent, modular control structures in the form of executable load modules that can be maintained in one or more libraries, and assembled

Art Unit: 2132

into control methods and models, and where such model control schemes can "evolve" as control information passes through the VDE installations of participants of a pathway of VDE content control information handling.

The advantage of Ginter et al. is then that it allows for electronic model to adapt with the changing needs and states of commercial applications and organizations.

It would have been obvious to one of ordinary skill in the art at the time of invention to employ the updating and modification mechanism of Ginter and to use VDE as a whole in order to allow a model of an organization to adapt to businesses or organizations as they evolve and change.

In reference to claim 17:

Lampson et. al. (Section 2. Concepts, page 268) discloses a system where at least one of said entities is an individual in an organization under "People: Lampson, Abadi"

In reference to claim 18:

Lampson et al. (Section 2. Concepts, page 268) discloses a system where at least one of said entities is a group of individuals in an organization.

In reference to claim 19:

Art Unit: 2132

Lampson et al. (Section 2. Concepts, page 268) discloses a system where at least one capability is a role in an organization.

In reference to claim 20:

Lampson et al. (Section 2. Concepts, page 268) discloses a system where at least one capability is a task in an organization.

In reference to claim 21:

Lampson et al. (Section 2. Concepts, page 268) discloses a system where at least one function is an operation by a functionary in an organization.

In reference to claim 22:

Lampson et al. (Section 2. Concepts, page 268) discloses a system where at least one function is an operation by a group of functionaries in an organization, where a group is a Principal and Principals may take on roles or "functions".

In reference to claim 23:

Lampson et al. (p. 269 4th paragraph and Section 5.2, p. 286-290) discloses a system where at least one of said characteristics and relationships is represented in a directory.

In reference to claim 25:

Art Unit: 2132

Lampson et al. (Figure 6, page 287) discloses a system where at least one of said characteristics and said relationships is represented in a public key infrastructure directory.

In reference to claim 26:

A system as in claim 16 where an operation of said system involves updating at least one directory.

The Examiner takes official notice that updating directories were well known at the time of invention.

For example, the deletion of a folder, and renaming of a folder in windows 95.

It would have been obvious to one of ordinary skill in the art at the time of invention to update a directory to allow a user to manage and maintain files within a computer.

In reference to claim 27:

Lampson et al. (Figure 6, page 287) discloses a system where said system's operations involve updating at least one public key infrastructure directory, where the authentication tree demonstrates the public key infrastructure directory.

Claim 28 is rejected for the updating and modification reasoning used in claim 16.

Claim 29 is rejected for the same reasons as claim 27.

Art Unit: 2132

In reference to claim 30:

Lampson et. al (p.283) discloses a system where said changing of the said maintained elements comprises change of databases, where the elements are principals and the credentials of an element are looked up in the database.

In reference to claim 31:

Lampson et. al (p.283) discloses a system where said changing of the said maintained elements comprises change of cryptographic certification information within the public key infrastructure directories and further database changes, where the elements are principals, and a change of cryptographic certification information would change the credentials of the element in the database.

In reference to claim 32:

Lampson et. al. (Section 5.1, 5.2, p.283-290) discloses a system where said entities, said characteristics and said relationships are maintained by combining database components and components of certification authorities of a public key infrastructure, where the entities are principals and their characteristics and relationships are maintained by combining information from the database (the credentials of the entities) and the certificates provided by the certification authorities of the public key infrastructure.

Art Unit: 2132

In reference to claim 33:

Lampson et. al. (p. 269 4th paragraph) discloses a system where said entities are represented in at least first directory, where the entities are principals and
"/com/dec/src/burrows and /com/dec/src/abadi" are first directories where the entities are represented
(Section 5.2, Path Names and Multiple Authorities, p. 287-290)
discloses a system where said characteristics and said relationships are represented in at least second directory, where the second directory is tree or directory of authentication, and the paths within the directory hold represent the cryptographic relationships between the entities.

Claim 34 is rejected for the same reason as claim 33.

In reference to claim 37:

Lampson et. al. (Section 5.1, A single certification authority, p. 283-286) discloses a system where said system's operation is activated by at least one designated entity amongst said entities, where the one designated entity is principal A, in first initiating the transaction.

In reference to claim 38:

Lampson et. al. (Section 5.1, A single certification authority, p. 283-286) demonstrates a system where said system's operation is activated based on agreed upon rules, where the agreed upon

Art Unit: 2132

rules are apparent in the operation of the users interacting with the certification authority.

As per claims 39 and 41,

Ginter et al. paragraphs 986, 1012, 1989, and 2006 discloses a method as in claim 1 wherein said method involves access control technology or the authorization rules as characteristics of relationships and the operation of the system is based on authorizations.

(986) In the example, subject table 462 associates users (or groups of users) with registered objects. The example subject table 462 performs the function of an access control list by specifying which users are authorized to access which registered VDE objects 300.

(1012) User or user group ID 472(2) identifies a user or a user group authorized to use the object identified in field 468(5). Thus, the fields 468(5) and 472(2) together form the heart of the access control list provided by subject table 462. User attributes field 472(3) may specify attributes pertaining to use/access to object 300 by the user or user group specified in fields 472(2). Any number of different users or user groups may be added to the access control list (each with a different set of attributes 472(3)) by providing additional subject records 470 in the "linked list" structure.

(1989) In this example, the law firm receives in VDE content containers documents from their client's VDE installation secure subsystem(s). Alternatively, or in addition, the law firm may receive either physical documents which may be scanned into electronic form, and/or they receive electronic documents which have not yet been placed in VDE containers. The electronic form of a document is stored as a VDE container (object) associated with the specific client and/or case. The VDE container mechanism supports a hierarchical ordering scheme for organizing files and other information within a container; this mechanism may be used to organize the electronic copies of the documents within a container. A VDE container is associated with specific access control information and rights that are described in one or more permissions control information sets (PERCs) associated with that container. In this example, only those members of the law firm who possess a VDE instance, an appropriate PERC, and the VDE object that contains the desired document, may

Art Unit: 2132

use the document. Alternatively or in addition, a law firm member may use a VDE instance which has been installed on the law firm's network server. In this case, the member must be identified by an appropriate PERC and have access to the document containing VDE object (in order to use the server VDE installation). Basic access control to electronic documents is enabled using the secure subsystem of one or more user VDE installations.

(2006) The organization as a whole may have a well-defined policy for access control to, and/or other usage control of documents. This policy may be based on a "lattice model" of information flow, in which documents are characterized as having one or more hierarchical "classification" security attributes 9903 and zero or more non-hierarchical "compartment" security attributes, all of which together comprise a sensitivity security attribute.

In reference to claim 40:

Ginter et al. (Figure 12, Item 730, Item 750, 744, 752) and paragraph 104

(104) Secondary storage 652 in this example stores code and data used by CPU 654 and/or SPU 500 to control the overall operation of electronic appliance 600. For example, FIG. 8 shows that "Rights Operating System" ("ROS") 602 (including a portion 604 of ROS that provides VDE functions and a portion 606 that provides other OS functions) shown in FIG. 7 may be stored on secondary storage 652. Secondary storage 652 may also store one or more VDE objects 300. FIG. 8 also shows that the secure files 610 shown in FIG. 7 may be stored on secondary storage 652 in the form of a "secure database" or management file system 610. This secure database 610 may store and organize information used by ROS 602 to perform VDE functions 604. Thus, the code that is executed to perform VDE and other OS functions 604, 606, and secure files 610 (as well as VDE objects 300) associated with those functions may be stored in secondary storage 652. Secondary storage 652 may also store "other information" 673 such as, for example, information used by other operating system functions 606 for task management, non-VDE files, etc. Portions of the elements indicated in secondary storage 652 may also be stored in ROM 658, so long as those elements do not require changes (except when ROM 658 is replaced). Portions of ROS 602 in particular may desirably be included in ROM 658 (e.g., "bootstrap" routines, POST routines, etc. for use in establishing an operating environment for electronic appliance 600 when power is applied).

Discloses the database maintenance operations involving said entities, characteristics and relationships.

Art Unit: 2132

In reference to claim 42:

Lampson et. al. (Section 5.2, Path Names and Multiple Authorities, p. 287-290) discloses a system where said characteristics and said relationships define authorization rules based on access structure, where the relationships defined by the authorization tree defines the authorization rules.

Claims 43 and 44 are rejected for the same reason as claim 42.

In reference to claim 45 and 46.

Ginter et al. (paragraphs 982, 983) discloses a system as in claim 16 with the additional operations of logging said system's operations.

(982) FIG. 28 shows an example of one possible detailed format for a receiving table 446. In one embodiment, receiving table 446 has a structure that is similar to the structure of the shipping table 444 shown in FIG. 27. Thus, for example, receiving table 446 may include a header 446a and a plurality of receiving records 447, each receiving record including details about a particular reception or scheduled reception of an administrative object. Receiving table 446 may include two linked lists, one for completed receptions and another for schedule receptions. Receiving table records 447 may each reference an entry within name services record table 452 specifying an administrative object sender, and may each point to an entry within administrative event log 442. Receiving records 447 may also include additional details about scheduled and/or completed reception (e.g., scheduled or actual date/time of reception, purpose of reception and status of reception), and they may each include validation tags for validating references to other secure database records.

(983) FIG. 29 shows an example of a detailed format for an administrative event log 442. In the preferred embodiment, administrative event log 442 includes an event log record 442(1) . . . 442(N) for each shipped administrative object and for each received administrative object. Each

Art Unit: 2132

administrative event log record may include a header 443a and from 1 to N sub-records 442(J)(1) . . . 442(J)(N). In the preferred embodiment, header 443a may include a site record number field 443A(1), a record length field 443A(2), an administrative object ID field 443A(3), a field 443A(4) specifying a number of events, a validation tag 443A(5) from shipping table 444 or receiving table 446, and a check sum field 443A(6). The number of events specified in field 443A(4) corresponds to the number of sub-records 442(J)(1) . . . 442(J)(N) within the administrative event log record 442(J). Each of these sub-records specifies information about a particular "event" affected or corresponding to the administrative object specified within field 443(A)(3). Administrative events are retained in the administrative event log 442 to permit the reconstruction (and preparation for construction or processing) of the administrative objects that have been sent from or received by the system. This permits lost administrative objects to be reconstructed at a later time.

In reference to claim 47:

Lampson et al. (p.286, 2nd paragraph) discloses a system with the additional operation of monitoring operations within a system, where a timestamp is well known in the art to be considered a monitoring operation.

In reference to claim 48:

Lampson et al. (p.286, 2nd paragraph) discloses a system with the additional operations of time stamping operations within said system.

In reference to claim 49:

Lampson et al. discloses a system of authentication in distributed systems where it is understood that at least one of said system's operations is performed distributedly via communication. Lampson et al. (Section 5.1, A single

Art Unit: 2132

certification authority, p. 283) specifically discloses contacting a certification authority as an operation performed distributedly.

In reference to claim 50:

Lampson et al. (p. 283) discloses a system where at least one of said system's operations is a distributed database operation.

In reference to claim 51:

Ginter et. al. (Figure 12a, paragraph 1655) discloses a system as in claim 16 where at least one of said system's operations involves physical handling of devices to one of said entities; where the physical handling is the client handling and using of a computer and a keyboard.

(1655) Each of electronic appliances 600(1), . . . 600(N) could comprise a different module of the same workstation device all contained within a common housing, or the different electronic appliances could be located within different system components. For example, electronic appliance 600(2) could be disposed within a disk controller unit, electronic appliance 600(3) could be disposed within a display device 614 housing, and the electronic appliance 600(N) could be disposed within the housing of a printer 622. Referring back to FIG. 7, scanner 626, modem 618, telecommunication means 624, keyboard 612 and/or voice recognition box 613 could each comprise a VDE electronic appliance 600 having its own SPU 500. Additional examples include RF or otherwise wireless interface controller, a serial interface controller, LAN controllers, MPEG (video) controllers, etc.

In reference to claim 52:

Lampson et. al. (Section 5.1, A single certification authority, p. 283 - 286) discloses database system representing a business

Art Unit: 2132

organization involving directories representing entities within said business organization, their characteristics, roles, and relationships together with their associations with cryptographic capabilities, the database system comprising following transactional components:

Connection to cryptographic authorities representing the cryptographic capabilities associated with said entities, said characteristics, and said relationships, where the cryptographic authorities are certification authorities, and the entities are principals who communication to the CA's in cryptographic transactions.

Lampson does not explicitly disclose:

- A maintenance system by which said database and said cryptographic authorities are maintained in coordination and by authorized parties assuring the representation of said organization and said cryptographic capabilities are soundly associated as defined by the coordination directives, where the maintenance of the authorizations is observed through the use of certification authorities, and using the database to check access control transactions.
- Maintenance transactions acting within said maintenance system, maintaining view representing an organization, where the maintenance transaction are database accesses to justify granting

Art Unit: 2132

Ginter et al. discloses an electronic embodiment of a system for control and maintenance of an operational structure including "changing the maintained electronic representation of said entities said characteristics and said relationships upon an addition, deletion or modification of a characteristic or relationship of the entities." paragraphs 164, 204, 209, 206.

Furthermore Ginter, on column 8, lines 1-7 discloses the following. " VDE normally employs an integration of cryptographic and other security technologies (e.g. encryption, digital signatures, etc.), **with other technologies including: component, distributed, and event driven operating system technology, and related communications, object container, database, smart agent, smart card, and semiconductor design technologies.**"

Ginter et al. is combined with Lampson for the same basis as previously recited in the rejection of claim 16.

In reference to claim 53:

Lampson et. al. (Section 2, p. 268 - 270) discloses a system wherein said organization comprises a plurality of entities, where entities are principals.

In reference to claim 54:

Lampson et. al (Section 5.2, Path Names and Multiple Authorities, p. 286-290) discloses a system wherein said cryptographic authorities is a plurality of at least one certification authorities.

Art Unit: 2132

In reference to claim 56:

Lampson et al. (Section 5.2, Path Names and Multiple Authorities, p. 286-290) discloses a system wherein said cryptographic authorities is a plurality of authorities organized hierarchically.

In reference to claim 57:

Lampson et al. (Section 9, Access Control, p. 305-307) discloses a system wherein said authorized parties are maintained by another instantiation of the system, where the other instantiation is the access control list.

In reference to claim 59:

Lampson et al. (Section 5.2, Path Names and Multiple Authorities, p. 283-286) discloses a system wherein said coordinating directives involve cryptographic fields assuring integrity of the operation, wherein the coordination of the entities with the certification authorities assure integrity of the operation

In reference to claim 61:

Lampson et. al. (p. 285) discloses a system wherein cryptographic capabilities involve digital certificates.

In reference to claim 62:

Lampson et. al. (Section 2, p. 268 - 270) discloses a system wherein said organization comprise various organizational units,

Art Unit: 2132

where the organization is the distributed authentication system, and the organizational units are defined as Concepts and other such units as principals, people, machines, services groups, all of which comprise an organization.

In reference to claim 63:

Lampson et. al. (Section 2 and Section 3.1,3.2, p. 268 - 272) discloses a system wherein said organization comprise of various organizational units where entities are defined in one unit and their roles are defined within a second unit, where the concept of Principals comprises entities, and the roles are defined in a second concept, in statements.

In reference to claim 66:

Ginter et al. (Figures 1 and 1A) discloses a method as in claim 16 where a plurality of entities are electronically visible to one part of the organization, a first set of outside viewers, or both, and roles or characteristics thereof are electronically visible to another part of the organization, a second set of outside viewers, or both, where the plurality of entities are visible to VDE participant 1, and participant N.

In reference to claim 67:

Ginter et al. (paragraph 1866) discloses a method as in claim 16 where maintaining of roles within the organizational structure is

Art Unit: 2132

protected and can be performed only by an authorized party inside or outside the organization, where the authorized party is the administrator.

(1866) Independent financial providers can play an important role in VDE 100. The VDE financial provider role is similar to the role played by organizations such as VISA in traditional distribution scenarios. In any distribution model, authorizing payments for use of products or services and auditing usage for consistency and irregularities, is critical. In VDE 100, these are the roles filled by independent financial providers. The independent financial providers may also provide audit services to content providers. Thus, budgets or limits on use, and audits, or records of use, may be processed by (and may also be put in place by) clearinghouses 116, and the clearinghouses may then collect usage payments from users 112. Any VDE user 112 may assign the right to process information or perform services on their behalf to the extent allowed by senior control information. The arrangement by which one VDE participant acts on behalf of another is called a "proxy." Audit, distribution, and other important rights may be "proxied" if permitted by the content provider. One special type of "proxy" is the VDE administrator 116b. A VDE administrator is an organization (which may be acting also as a financial clearinghouse 116) that has permission to manage (for example, "intervene" to reset) some portion or all of VDE secure subsystem control information for VDE electronic appliances. This administration right may extend only to admitting new appliances to a VDE infrastructure and to recovering "crashed" or otherwise inoperable appliances, and providing periodic VDE updates.

Conclusion

8. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a)

Art Unit: 2132

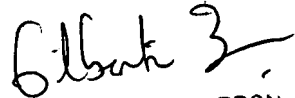
will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA
S.L.
08/26/2007


GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100